The Cyber Winter of Discontent

An Analysis of Russia’s Winter Cyberwarfare Campaigns targeting Critical National Infrastructure in Ukraine and the West and Assessment for Winter 2023/2024

Roman Faithfull Cyber Intelligence Lead
Introduction

Russia invaded Ukraine on 24 February 2022, meaning Ukraine has so far endured two winters at war. By the time this white paper is released, the country will be in its third. Winter is commonly thought of as a time where combat operations see a pause, or at least a lull in intensity. Freezing conditions cause logistical challenges, making it harder to keep troops warm, fed, motivated, and supplied with sufficient materiel to retain the initiative. Belligerents therefore often use Winter to conduct offensive campaigns less affected by the inclement weather, such as cyber, disinformation, and other types of so-called hybrid warfare.

As such, Russia will almost certainly seek to continue leveraging its cyberwarfare capabilities to target Ukraine’s critical national infrastructure (CNI) at a time when the country’s energy grid, telecommunications, hospitals, industry, and government institutions, will already be under heavy strain.

Since the start of the war, Ukraine’s CNI has suffered most from Russian cyberattacks. These have targeted the logistics, health care, agricultural and retail sectors, making it more difficult for Ukraine to produce and distribute food and medicine to its population. Frequent attacks against media, telecommunications and internet providers make it harder for the country to keep its populace well informed about kinetic attacks. Those conducted against Ukraine’s energy providers and storage facilities undermine its ability to keep its population warm and able to work.

However, Russia’s Winter cyberwarfare campaigns have so far certainly not limited their scope to only targeting Ukraine-based entities; they have frequently affected CNI organisations in the countries that support it. At present, the two belligerents are locked in a situation of “positional warfare”, with neither side able to take large swathes of territory as they were during previous phases of the war. As Russia finds itself continuing to struggle on the battlefield with issues such as manpower and morale, it has in turn increasingly turned to its cyberwarfare capabilities to make an impact on the overall conflict.

This white paper will provide an overview of Russia’s previous Winter cyber campaigns against the CNI of Ukraine and its allies. It will address how Russia may seek to target Ukrainian and Western CNI to prevent Ukraine from meeting the conditions necessary to overcome positional warfare.
Russia launched a number of cyberattacks against CNI in Ukraine both immediately prior to, during, and immediately following its land-based invasion on 24 February 2022. However, it is important to note that Russia had been frequently targeting Ukraine’s CNI ever since it illegally annexed Crimea in 2014. In June 2017, in attacks widely attributed to Russia, NotPetya wiper malware was used to destroy data and take systems offline at the Chornobyl nuclear power plant; this also affected almost 13,000 devices used by other public institutions, banks, postal services, newspapers, transport infrastructure, and businesses in Ukraine. These attacks were not contained to Ukraine; they spilled out to affect CNI in Europe and North America, causing over US$10 billion in losses. The attacks intensified in severity and frequency leading up to the 2022 invasion.

Immediately prior to and immediately following the outbreak of war, Russia’s cyberattacks against Ukrainian CNI primarily targeted government, media, and communications networks and infrastructure. They had the goal of sowing panic and confusion amongst the populace and making it more difficult for the Ukrainian government to effectively coordinate a united and coherent response. These attacks were frequently launched in tandem with simultaneous kinetic actions and attacks.

Prior to the invasion

Ukraine’s CNI was routinely targeted in the months prior to the invasion using a variety of different techniques consistent with Russia’s previous cyber and hybrid-warfare campaigns. In January 2022, the country saw defacement attacks against the websites of over 70 government agencies, including those responsible for defence, foreign affairs, education, and science. The attackers, later assessed to be Russian, masqueraded as Polish, replacing the content on sites with messages intended to enflame anti-Polish sentiment in Ukraine. Russia also targeted several non-profit and IT organisations the same month with wiper malware that was disguised as ransomware. On 15 February, the websites of the Ministry of Defence, Army, and Ukraine’s two largest banks were taken down in a large DDoS attack. This affected the mobile apps and ATMs of the banks and was described as “the largest assault of its kind in the country’s history.”

The day before the invasion the websites for various governmental, financial, and media organisations were taken offline in DDoS attacks. The same day, over 100 Ukrainian organisations in the financial, IT and aviation sectors were hit by the data wiper HermeticWiper. This coincided with the Russian recognition of separatist regions in eastern Ukraine and the authorisation of Russian troop deployments there. An hour before the invasion began in earnest, Russia launched an attack against Ukraine’s Viasat KA-SAT satellite network, which led to communication outages for individuals and public and private Ukrainian entities. This was likely intended to disrupt the country’s military networks, which relied heavily on Viasat for communications.
Following the invasion

Russian used similar tactics following its invasion in February 2022. The use of wiper malware was a prominent feature, with IssacWiper deployed against Ukrainian government websites on 25 February. On 27 February, a border control station was struck with Russian wiper malware, which prevented refugees from crossing into Romania. These attacks continued into March 2022, with CaddyWiper heavily deployed against government and financial organisations.

There were few attacks against CNI in the West in Winter 2021/2022 during the initial stages of the war, though some attacks principally targeting Ukraine did spill into Europe; the 24 February 2022 attack on Viasat deactivated the satellite modems of wind turbines based in Germany. Noting this, and acknowledging that large-scale attacks could spill into other countries as they had done before the invasion, in March 2022 US President Joe Biden urged US business leaders to harden the cybersecurity posture of their organisations. Leaders in the EU issued similar advisories, noting that Russia’s potential threat to organisations went beyond Ukraine.

Analysis

Despite the scale and intensity of these attacks, researchers have assessed that Russia’s offensive cyberwarfare campaign did not go as successfully as the Kremlin will have hoped. Though many key networks supporting Ukrainian CNI were taken down, they did not stay offline for sufficient time; Ukrainian communication infrastructure was still running five days after the invasion, which allowed the government to coordinate a successful defence of Kyiv. Russia’s failures, and Ukraine’s successes, on the cyber frontlines are likely due to a number of factors.

Firstly, mirroring its struggles in its conventional military campaign, Russia underestimated Ukraine’s defences. Due to Russia’s near-incessant targeting of Ukraine in the build-up to the invasion and before, Ukraine had ample opportunities to learn from its enemy and prepare its cyber defences. In response to the January attacks, NATO further increased its coordination with Ukraine, and later signed an agreement that granted the country access to its malware information sharing platform. This almost certainly helped Ukraine better contain the threat from Russia’s oft-used wiper malware, which did not achieve the same impact as in previous campaigns. Furthermore, on the day of the invasion, Ukraine requested that the EU activate PESCO’s Cyber Rapid Response Teams, the first time this had occurred in an operational context. This undoubtedly provided it with greater visibility into Russian cyberattacks and helped advise decision makers at Ukrainian CNI entities on how to contain the threats to their organisations.

Secondly, the country’s government reacted swiftly to address the vulnerabilities that had been exposed in the initial attack. Recognising that its domestically-hosted internet and communication systems, such as Viasat, were vulnerable to cyber and kinetic attacks, the Ukrainian government appealed to US-based aerospace and technology company Space X to provide it with access to the Starlink satellite internet constellation. The first Starlink terminals arrived on 28 February and provided much needed resilience to Ukraine’s communication infrastructure; Russia would have to conduct kinetic attacks on Space X’s satellites if it wanted to take down Starlink, which would risk bringing the US and/or other countries into the war.

Russia underestimated Ukraine’s defences. Due to Russia’s near-incessant targeting of Ukraine in the build-up to the invasion and before, Ukraine had ample opportunities to learn from its enemy and prepare its cyber defences.
Ukraine also quickly began conducting counter-offensive cyber operations of its own, announcing the creation of The IT Army of Ukraine on 26 February 2022, which leveraged the expertise of civilian cyber specialists. In the months following the invasion, Ukraine would strengthen its cooperation with NATO, the EU and the US to shore up its cyber defence and intelligence gathering capabilities.

Following Russia’s failure to capture Kyiv and enact regime change early in 2022, it continued with its attempts to annex the country, seizing and occupying Ukrainian lands in the Northeast, East, South, and Southwest. However, in September 2022, Ukrainian forces, using recently acquired materiel donated by its Western allies, liberated vast swathes of Russian-occupied territory in Kharkiv oblast. Then, in November, it routed Russian forces in Kherson city and on the east bank of the Dnipro River, bringing much of Kherson oblast back under Ukrainian control. Though by now Ukraine’s offensive cyber capabilities were much more advanced, Russia would continue its targeting of Ukrainian CNI into the Winter. By this time, it had also begun targeting the CNI of Ukraine’s allies. Aside from this, there were some other noticeable changes.

The most notable difference between the Winter of 2022/2023 and Russia’s cyber campaign against CNI the previous Winter, was the greater and growing involvement of pro-Kremlin hacktivist groups. These leveraged large botnets to conduct DDoS attacks and mainly coordinate their actions through instant messaging platforms such as Telegram and dedicated cybercriminal forums. Though it is unclear the extent to which the Kremlin may influence, sponsor, or directly control these groups, they have formed a key component of Russia’s attacks against CNI; by Winter 2022/2023 DDoS attacks constituted the most common form of attack. The increase of Russia’s use of hacktivist groups is likely due to several factors.

Firstly, it is likely that Russia had used up a significant portion of its attack resources in the opening stage of the war. Its cyber campaign against Ukraine has been described by the UK’s National Cyber Security Centre as “probably the most sustained and intensive … on record”. It almost certainly had a stockpile of compromised remote initial accesses, novel malware, and zero-day exploits that it deployed. On the opening day of the invasion, Russia successfully deployed more destructive malware than the rest of the world’s cyber powers combined typically use in a given year.
attacks and react accordingly, adapting to the threat they pose. These
offensive resources are no longer available to Russia in the same quantity
and with the same element of surprise.44

Secondly, midway through 2022, Russia began to experience a shortage of
IT specialists, as many began fleeing the country to avoid the draft. Russia’s
Ministry of Internal Affairs reported that approximately 170,000 IT workers
had left by June 2022,45 and it is almost certain that more followed in the
months after.

These two factors combined explain the rise of pro-Kremlin groups and
their DDoS attacks. Hacktivist collectives can operate from anywhere in the
world – it is likely that many pro-Russian hacktivists operate from outside of
Russia – and DDoS attacks have relatively low operating costs and barriers
to entry, especially in comparison to creating and deploying novel malware
or zero-day exploits.

**Attacks against Ukraine**

Russia heavily targeted Ukrainian CNI in Winter 2022/2023, with the top
targeted sectors being public administration, financial services, media,
technology, transportation, and energy.46 On 3 December 2022, pro-Kremlin
hacktivist group NoName05716 claimed responsibility for a three-day DDoS
campaign against the servers of a Ukrainian telecommunications company,
disrupting citizens’ access to the company’s online resources. In mid-January 2023, CaddyWiper reappeared alongside ZeroWipe (Windows),
SDelete (Windows), AwfulShred (Linux), and BidSwipe (FreeBSD) wiper
malware, targeting the information and communication system of the
Ukrainian National Information Agency (Ukrinform).47 This was not an
opportunistic attack; the attackers had gained remote access to Ukrinform’s
network on 7 December and waited more than a month before attempting
to execute the malware. However, this attack was only partially successful
and was largely contained before significant damage occurred.48 Ukraine
attributed the attacks to Russia’s state-sponsored advanced persistence
threat (APT) group Sandworm, part of Russian Military Unit 74455 of the
Main Intelligence Directorate (GRU).49

February 2023 was a particularly prominent month, with pro-Kremlin threat
actors conducting 62% of all recorded attacks in Q1 2023.50 This is likely due
to the month coinciding with the one-year anniversary of the initial invasion.
On 21 February 2023, Russia targeted Ukrainian state agencies with the
Remcos remote access trojan (RAT).51
Attacks against the rest of the world

By Winter 2022/2023 Russia had massively increased the number of attacks against Ukraine’s allies. The CyberPeace Institute documented 475 incidents affecting entities in the West in 2023 Q1 alone, compared to 461 throughout the whole of 2022.52 As with attacks against Ukraine, the vast majority of incidents recorded were DDoS attacks.53 CNI was heavily targeted, with public administration, transportation, and financial services most commonly affected. Poland, the US, and Germany were the most popular targets of Russian attacks, with Latvia, Sweden, Slovakia, Japan, Spain, Italy, Denmark, and Norway also featuring prominently.54

On 15 December 2022, NoName05716 claimed responsibility for a confirmed DDoS attack against the website of the lower house of Poland’s parliament, resulting in temporary inaccessibility.55 By February 2023, Poland was reportedly being targeted in a cyberattack every nine minutes.56 These were affecting private organisations as well as hospitals, medical institutions, banks, and government agencies.

On 7 January 2023, Norwegian shipping company DNV reportedly suffered a ransomware attack on its ShipManager servers that affected approximately 1,000 vessels worldwide. Though this attack could not be definitively attributed to Russia, it is well known that ransomware operations affecting the West frequently originate from groups that are aligned with the Kremlin’s interests.57 On 28 January 2023, pro-Kremlin hacktivist group Anonymous Sudan claimed responsibility for a confirmed DDoS campaign against 19 hospitals based in the Netherlands, successfully taking down their websites.58

Analysis

It is likely that Russia’s expansion of the scope of its cyberattacks to include the CNI of Ukraine’s allies in Winter 2022/2023 reflected Moscow’s failures on the battlefield in 2022. Ukraine’s progress in Kharkiv and Kherson relied heavily on military materiel donated by its allies,59 particularly the US60 in the Spring and Summer of that year. Researchers have assessed that Russia acknowledged it would not have the industrial capacity to maintain superiority or parity with Ukrainian military capabilities if Kyiv’s military-industrial complex continued to ramp up production of domestic materiel production and Ukraine’s allies continued to supply it.61

Russia’s change of targeting almost certainly reflected an acknowledgement that it needed to stop Western materiel from getting into Ukraine and then reaching the front lines. Thus, Russia’s attacks against CNI had three aims, in parallel with its overall strategic aim of causing “war fatigue” via hybrid warfare in countries which had donated or had pledged to donate weapons to Ukraine.

Firstly, Russia sought to target CNI in Ukraine’s allies to influence domestic populations to pressure their governments to either stop providing financial or military assistance to the country, or to persuade Ukraine to come to the negotiating table with Russia to end the war.65 In this way, attacks against CNI would produce the greatest visibility amongst domestic populations due to their greater proportional impact on the populace.

Secondly, Russia aimed to target European CNI, particularly the German banking sector and the logistics sectors in Ukraine’s close neighbours Poland and Latvia, to increase the difficulty of processing financial aid to Russia.
The Cyber Winter of Discontent

Current situation in Russia and Ukraine going into Winter 2023/2024

As we move into Winter 2023/2024, much has changed. 2023 saw Finland become the 31st member of NATO in April, with Sweden’s membership also becoming ratified in all but name. Significant geopolitical events occurred. The demise of the leader of Russian private military contractor Wagner, Yevgeny Prigozhin, following his aborted coup on Moscow, has threatened Russia’s neo-imperialist campaigns in Africa and Latin America. Conflict breaking out between Palestine and Israel in October has taken some attention away from the war in Ukraine. Domestically, Russian authorities are grappling with somewhat of an identity and manpower crisis ahead of Putin’s potential 2024 election. Ukraine has also suffered setbacks, as the head of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and his deputy were dismissed in late November following probes into corruption at their organisation.

Positional warfare

At present, the conflict in Ukraine has moved into a more stagnant phase, though despite the renewed use of trench warfare, this is not akin to the stalemate seen on the Western front in the First World War. On 1 November 2023, Ukrainian Commander-in-Chief General Valerii Zaluzhnyi published an essay titled “Modern Positional Warfare and How to Win It” in which he outlined the conditions Ukraine must achieve to overcome the current “positional” stage of the war and regain the offensive. Positional warfare refers to military operations that do not result in rapid or dramatic territory changes despite the continuous efforts of both sides to improve them. Fighting on the ground has crystallised around four key areas in the East, South, and Southeast of Ukraine, with Bakhmut, Avdiivka, Robotyne, and a Ukrainian bridgehead on the west bank of the Dnipro around Kherson experiencing intense fighting but few positional changes in recent months. Indeed, Russia has seen huge losses of men and materiel primarily in trying to take the small city of Avdiivka, losing hundreds of armoured vehicles that would exhaust the entire stocks of most nations.
Broadly, Zaluzhnyi’s conditions for overcoming positional warfare were: gaining air superiority, breaching mine barriers in depth, increasing the effectiveness of counter-battery, creating and training the necessary reserves, and building up electronic warfare (EW) capabilities. Zaluzhnyi’s essay received considerable attention from the Russian milblogger community, with many acknowledging that Moscow must stop these conditions from being met if it is to win the war. Russia will have noted that a key factor in meeting these conditions will be the ability and motivation of Ukraine’s allies to continue providing financial and materiel assistance to the country. As such, it has continued both kinetic and cyberattacks against Ukraine’s CNI throughout 2023, both to increase war fatigue in the West and to hamper domestic arms production and supply to the front lines. It will continue these attacks going into Winter 2023/2024. It should be noted that Russia will almost certainly massively target Western domestic audiences with disinformation campaigns, especially in the context of upcoming European and US elections, to attempt to ensure candidates more favourable to Russian narratives are elected. However, whilst extremely significant, this falls outside the scope of this report.
Predictions

Cyberwarfare will continue to form a key part of Russia’s campaign against Ukrainian and Western CNI as it seeks both to prevent Ukraine from meeting the conditions necessary to overcome positional warfare as described by Zaluzhnyi ahead of the more favourable weather conditions of Summer 2024, and to present the current administration in a more favourable light in view of the upcoming potential Russian presidential elections in March 2024.

As mentioned, Russia will strongly desire to attack CNI in Ukraine and its allies. However, its missile production is struggling to keep pace with its tactical, operational, and strategic usage. This is due to increasing EU and NATO sanctions, which directly affect Russia’s military industrial complex’s ability to produce these complex weapon systems. Russia’s domestic economic and migration woes are also likely impeding production. Russia is currently trying to balance its pressing need to conscript economic migrants to fight in Ukraine as ultra-nationalists complain about rising economic migration into the country against the backdrop of a shortage of workers in sectors that could be filled with these migrants. The Kremlin frequently presents contradictory and conflicting positions on the status of migrants in the country. Even once missiles that could destroy CNI in Ukraine are produced, more and more Western-supplied Ukrainian short-, mid-, and long-range anti-air systems are coming online in Ukraine, which increases the rate at which Russian kinetic attacks are thwarted.

As such, Russia will likely continue to leverage its cyberwarfare capabilities to target CNI, probably with heavy use of wiper malware. Cyber espionage may also be a key aim, as Moscow seeks to intercept communications and sensitive data relating to advanced technologies that are moving into the country. However, it is realistically possible that Russia is starting to struggle to produce novel and effective malware due to a growing shortage of cyber professionals in the country, combined with the continual strengthening of Ukraine’s cyber defences. As with military materiel, offensive cyber capabilities take time, resources, and expertise to produce. Indeed, Ukraine has reported that Russia increasingly targeted victims in the cybersphere opportunistically, rather than selectively attacking specific organisations, likely having used up most of its pre-war non-reserve resources.

As with kinetic reserves, Russia would likely choose to keep some cyberattack resources in reserve rather than exhausting them all during this war, to ensure that they retain offensive and defensive capability should they be invaded themselves; Moscow would likely stop conducting cyberattacks long before it actually exhausted its capability to carry them out.
It is therefore realistically possible that Russia will increasingly target the CNI of Ukraine’s allies leading into 2024 and beyond; it is likely cyber defences outside of Ukraine have remained comparatively weak as they have not been so heavily targeted in comparison to those of Ukraine.

Hacktivism will also almost certainly remain a key component of Russia’s campaigns against Ukrainian and Western CNI, due to its low operational cost and the level of plausible deniability these groups afford the country should they decide to increase the rate and intensity of their attacks against targets outside of Ukraine.

However, in recent months, Cyjax has observed many pro-Kremlin hacktivist collectives switching their targeting away from Ukraine to attacks on organisations based in Israel and those countries supporting it. This is in line with Vladimir Putin’s increasingly anti-Israeli rhetoric as he attempts to demonstrate the supposed hypocrisy of the West’s condemnation of Russia’s invasion of Ukraine. It is likely that, should Russia continue to suffer losses on the battlefield, the focus of its cyber campaigns will increase back to Ukraine and its allies, and CNI is a key target.
Concluding remarks

As we move into Winter 2023/2024, Russian cyberattacks against the CNI in Ukraine and its allies have become increasingly important to its strategic goals. However, it appears that Russia’s attacks in this regard so far have not had the desired effect: the West is still supplying Ukraine with financial aid and materiel, and Ukraine continues to be able to move this across the country to support its strategic, operational and tactical aims. Russia has thus far seen diminishing returns on its investments into cyberwarfare, and cyber operations against CNI will likely play a supporting, rather than decisive, role in Ukraine. Russia will probably see much more success via disinformation campaigns aimed at destabilising the West’s desire to continue supporting its ally in the medium to long term, and Moscow may therefore choose to invest more of its dwindling resources into funding this area of attack.
Endnotes

28. https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence
The Cyber Winter of Discontent

33 https://reason.com/video/2022/03/05/can-elon-musks-starlink-keep-ukraine-online/
37 https://www.euam-ukraine.eu/
40 https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward
48 https://www.gov.pl/web/special-services/russian-cyberattacks
51 https://nltimes.nl/2023/01/31/hospitals-cybersecurity-firm-also-targeted-pro-russia-cyberattack
52 https://eur-lex.europa.eu/eli/dir/2022/2555/oj
53 https://kclpure.kcl.ac.uk/ws/portalfiles/portal/224102580/Lessons_from_the_Russo_Ukrainian_conflict_the_primacy_of_logistics_over_strategy.pdf
56 https://therecord.media/royal-dirkzwager-ransomware-attack-dutch-shipping
57 https://eur-lex.europa.eu/eli/dir/2022/2555/oj
58 https://kclpure.kcl.ac.uk/ws/portalfiles/portal/224102580/Lessons_from_the_Russo_Ukrainian_conflict_the_primacy_of_logistics_over_strategy.pdf
The Cyber Winter of Discontent

71 https://www.csis.org/analysis/post-prigozhin-russia-africa-regaining-or-losing-control
72 https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-6-2023
75 https://www.youtube.com/watch?v=WAmapFtQvXs
76 https://infographics.economist.com/2023/ExternalContent/ZALUZHNYI_FULL_VERSION.pdf
77 https://twitter.com/DefenceHQ/status/1729060117235028273
79 https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-7-2023
80 https://www.youtube.com/watch?v=ctrtAwT2sgs
81 https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-6-2023
83 https://www.economist.com/europe/2023/10/24/ukraines-allies-are-scrambling-to-bolster-its-air-defences
84 https://www.washingtonpost.com/world/2023/05/19/ukraine-air-defense-systems-patriot/
85 https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
86 https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward
87 https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-22-2023
About Cyjax

CYJAX is a threat intelligence provider dedicated to increasing business's resilience in the face of evolving threats. Our strategic approach prioritises depth over breadth, allowing us to deliver highly tailored solutions seamlessly integrated into your existing tech stack. We cut costs and noise, simplifying the complex cybersecurity world. We’ve successfully protected businesses across industries, including Fortune 500 companies. Our mission is to fortify resilience and ensure your organisation thrives in today’s interconnected world.

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com